(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－92783
（P2001－92783A）
(43)公開日　平成13年４月６日(2001.4.6)

(51)Int.Cl.[7]	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
1/00	３７０	1/00	３７０Ｅ	

審査請求　未請求　請求項の数３　ＯＬ　（全 14 頁）

(21)出願番号　特願平11－271848

(22)出願日　平成11年９月27日(1999.9.27)

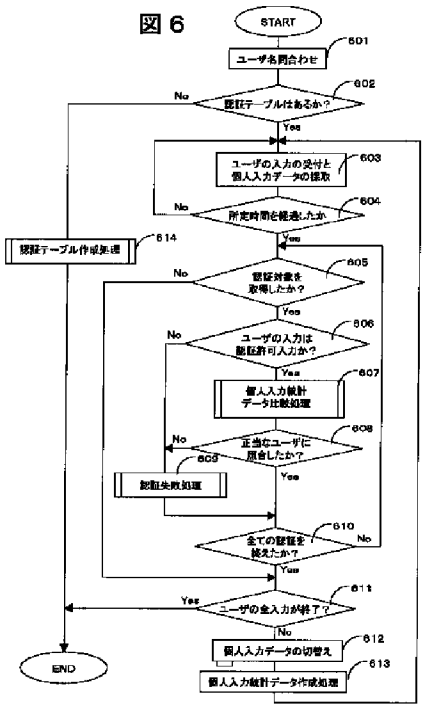
(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地
(72)発明者　小林　伸嘉
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウエアエンジニアリング株式会社内
(74)代理人　100083552
弁理士　秋田　収喜

Ｆターム(参考)　5B085 AE15 AE23

(54)【発明の名称】　個人認証方法およびシステム、記録媒体

(57)【要約】
【課題】　認証済みの正規ユーザが離席したような場合であっても、不正な第３者による不正使用を抑止することができる個人認証方法およびシステムを提供すること。
【解決手段】　目的とする結果を得るに至る前記入力手段の操作手順、操作態様、操作環境少なくとも１つを個人別ファイルに収集し蓄積するステップと、コンピュータシステムの使用許可を得ようとするユーザ名またはパスワードの入力に対し、所定の監視間隔で前記入力手段の操作手順、操作態様、操作環境を監視し、その監視期間中において収集したデータと事前に前記個人別ファイルに蓄積しておいたデータとを比較し、両者の差異が許容範囲内でなければ不正ユーザとして認定し、コンピュータシステムまたは該コンピュータシステムに付属する資源の使用を抑止するステップとを備えることを特徴とする。

図６



1

【特許請求の範囲】

【請求項１】　ユーザが操作する入力手段として、少なくともキーボードおよびポインティングデバイスを備えるコンピュータシステムにおける個人認証方法であって、

目的とする結果を得るに至る前記入力手段の操作手順、操作態様、操作環境の少なくとも１つを個人別ファイルに収集し蓄積するステップと、

コンピュータシステムの使用許可を得ようとするユーザ名またはパスワードの入力に対し、所定の監視間隔で前記入力手段の操作手順、操作態様、操作環境の少なくとも１つを監視し、その監視期間中において収集したデータと事前に前記個人別ファイルに蓄積しておいたデータとを比較し、両者の差異が許容範囲内でなければ不正ユーザとして認定し、コンピュータシステムまたは該コンピュータシステムに付属する資源の使用を抑止するステップとを備えることを特徴とする個人認証方法。

【請求項２】　ユーザが操作する入力手段として、少なくともキーボードおよびポインティングデバイスを備えるコンピュータシステムにおいて、

目的とする結果を得るに至る前記入力手段の操作手順、操作態様、操作環境の少なくとも１つを個人別ファイルに収集し蓄積する手段と、

コンピュータシステムの使用許可を得ようとするユーザ名またはパスワードの入力に対し、所定の監視間隔で前記入力手段の操作手順、操作態様、操作環境の少なくとも１つを監視し、その監視期間中において収集したデータと事前に前記個人別ファイルに蓄積しておいたデータとを比較し、両者の差異が許容範囲内でなければ不正ユーザとして認定し、コンピュータシステムまたは該コンピュータシステムに付属する資源の使用を抑止する手段とを含む個人認証処理手段を備えることを特徴とするコンピュータシステム。

【請求項３】　ユーザが操作する入力手段として、少なくともキーボードおよびポインティングデバイスを備えるコンピュータシステムにおける個人認証処理用プログラムを記録した記録媒体であって、

目的とする結果を得るに至る前記入力手段の操作手順、操作態様、操作環境の少なくとも１つを個人別ファイルに収集し蓄積する処理と、

コンピュータシステムの使用許可を得ようとするユーザ名またはパスワードの入力に対し、所定の監視間隔で前記入力手段の操作手順、操作態様、操作環境の少なくとも１つを監視し、その監視期間中において収集したデータと事前に前記個人別ファイルに蓄積しておいたデータとを比較し、両者の差異が許容範囲内でなければ不正ユーザとして認定し、コンピュータシステムまたは該コンピュータシステムに付属する資源の使用を抑止する処理とを含むコンピュータが読み取り可能なプログラムが記録されていることを特徴とする記録媒体。

2

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータシステムを使用するユーザの個人認証方法およびシステムに関するものである。

【０００２】

【従来の技術】従来、コンピュータシステムの個人認証方法に関する技術として、予め個人認証情報をコンピュータが読み取り可能な記録媒体（フロッピー（登録商標）ディスクなど）に記憶し、個人認証情報の入力を明示的にユーザに要求し、入力されたデータとコンピュータに記憶されている個人認証情報との比較によって個人認証を行う方法が挙げられる。例えばコンピュータを使用するときに、ユーザにパスワードの入力を促す画面を表示し、入力されたパスワードと予め設定されているパスワードとの比較を行い、同じであればコンピュータの使用を許可することとしていた。また、指紋や音声などの身体情報を記憶しておき、コンピュータを使用するときに、ユーザに指紋読取装置や音声入力装置に入力を促す画面を表示し、入力された身体情報と予め設定されている身体情報との比較を行い、同じであればコンピュータの使用を許可することとしていた。

【０００３】

【発明が解決しようとする課題】しかしながら、上記従来技術を用いた個人認証方法では、予め設定されているパスワード等の個人認証情報がわかれば誰でも特定の個人として個人認証を受けることができ、不正な第３者による不正使用を抑止することができないという問題がある。また、指紋などの身体情報を入力するためには、指紋入力装置などの特別の入力装置が必要となり、コストが嵩むという問題がある。特に、個人認証を受けた状態で認証済みの正規ユーザが離席すると、他人がそのコンピュータを操作することが可能になる。本発明の目的は、認証済みの正規ユーザが離席したような場合であっても、不正な第３者による不正使用を抑止することができる個人認証方法およびシステムを提供することにある。

【０００４】

【課題を解決するための手段】上記目的を達成するために、本発明は、ユーザが操作する入力手段として、少なくともキーボードおよびポインティングデバイスを備えるコンピュータシステムにおける個人認証方法であって、目的とする結果を得るに至る前記入力手段の操作手順、操作態様、操作環境の少なくとも１つを個人別ファイルに収集し蓄積するステップと、コンピュータシステムの使用許可を得ようとするユーザ名またはパスワードの入力に対し、所定の監視間隔で前記入力手段の操作手順、操作態様、操作環境を監視し、その監視期間中において収集したデータと事前に前記個人別ファイルに蓄積しておいたデータとを比較し、両者の差異が許容範囲内

でなければ不正ユーザとして認定し、コンピュータシステムまたは該コンピュータシステムに付属する資源の使用を抑止するステップとを備えることを特徴とする。

【０００５】また、ユーザが操作する入力手段として、少なくともキーボードおよびポインティングデバイスを備えるコンピュータシステムにおいて、目的とする結果を得るに至る前記入力手段の操作手順、操作態様、操作環境の少なくとも１つを個人別ファイルに収集し蓄積する手段と、コンピュータシステムの使用許可を得ようとするユーザ名またはパスワードの入力に対し、所定の監視間隔で前記入力手段の操作手順、操作態様、操作環境の少なくとも１つを監視し、その監視期間中において収集したデータと事前に前記個人別ファイルに蓄積しておいたデータとを比較し、両者の差異が許容範囲内でなければ不正ユーザとして認定し、コンピュータシステムまたは該コンピュータシステムに付属する資源の使用を抑止する手段とを含む個人認証処理手段を備えることを特徴とする。

【０００６】

【発明の実施の形態】以下、本発明を実施する場合の一形態を図面を参照して具体的に説明する。図１に、本発明の実施の一形態のコンピュータシステムを示す。この実施形態のコンピュータシステムは、入力装置１０、演算装置２０、制御装置３０、出力装置４０、記憶装置５０とから構成されている。

【０００７】入力装置１０は、データを入力する装置である。入力装置１０は、対話型形式入力装置、シート型形式入力装置とその他の入力装置に分けられる。対話型入力装置として、キーボード、音声入力装置、ポインティングデバイス（マウス）等がある。シート形式入力装置として、光学式文字読取装置や光学式マーク読取装置等がある。その他の入力装置としてバーコードリーダーやイメージスキャナ等がある。キーボード１０１は、ユーザがキーと呼ばれるボタンを押す事で文字や数字を入力するための入力装置である。マウス１０２は、ユーザが机などの上で動かすことにより移動方向と移動量を検出し、コンピュータに入力するための複数のボタンのついた入力装置である。演算装置２０は、コンピュータにおいて算術演算や論理演算を行う装置である。制御装置３０は、コンピュータ上の他の装置を制御する装置である。出力装置４０は、コンピュータ上のデータを出力する装置である。出力装置は、対話形式出力装置と、シート形式出力装置に分けられる。対話形式出力装置として、ディスプレイや音声出力装置等がある。シート形式出力装置として、プリンタやプロッタ等がある。記憶装置５０は、コンピュータのデータやプログラムを記憶する装置である。記憶装置５０は、主記憶装置と補助記憶装置に分けられる。また、制御装置３０と演算装置２０、主記憶装置を合わせて処理装置という。記憶装置５０には、個人入力データ５０１を記憶する領域（ファイル）が確保されている。

【０００８】個人入力データ５０１は、目的とする結果を得るに至る入力装置１０における操作手順、操作態様、操作環境を個人別に収集して蓄積しておくためのものである。この個人入力データ５０１は、１つのコンピュータシステムを１人のみで使用する場合には１つのみ作成されるが、複数人で共用する場合にはその人数分だけ作成される。

【０００９】本発明においては、コンピュータシステムの使用許可を得ようとするユーザ名またはパスワードの入力に対し、所定の監視間隔で入力装置１０における操作手順、操作態様、操作環境の少なくとも１つを監視し、その監視期間中において収集したデータと事前に収集・蓄積しておいた個人入力データ５０１とを比較し、両者の差異が許容範囲内でなければ不正ユーザとして認定し、コンピュータシステムまたは該コンピュータシステムに付属する資源の使用を抑止することを特徴とするものである。

【００１０】ここで、コンピュータシステムに付属する資源とは、記憶装置、出力装置、プログラム、外部のネットワークなどを全て含むものであり、抑止の対象となる資源はコンピュータシステムの正規ユーザによって予め設定可能であり、全てを抑止する場合と、一部を抑止する場合がある。

【００１１】本発明においては、入力装置１０における操作手順、操作態様、操作環境を監視していることを正規および不正ユーザのいずれにも意識させないように、入力装置１０における操作手順、操作態様、操作環境のデータを収集するようにしている。

【００１２】ここで、操作手順とは、後述するように、キーボードによって文字を入力する場合に、例えば「し」を入力する場合に、「ＣＩ」と入力するか、「ＳＨＩ」と入力するかといったキー操作手順のことである。また、操作態様とは、例えばページ切替えを行う場合に、ページ切替えのアイコンをマウス操作で行うか、ファンクションキー操作で行ったかというように、目的とする結果を得るに至るまでの入力手段の使い方のことである。また、操作環境とは、例えばネットワークを介して情報を収集する場合に、情報源を一覧表示しておいた環境で所望の情報源を指定したか、一覧表示しないで情報源のＵＲＬアドレスを直接指定したかなど、入力装置を用いる環境のことである。本発明は、個人によって、このような操作手順、操作態様、操作環境に個性があることに着目し、この個性を利用して正規のユーザであるか否かを認証するものである。

【００１３】なお、キー操作のリズムを監視し、そのリズムの相違によって認証を行う方法（特開平１１－１５９００号）があるが、キー操作の習熟度やユーザの体調によってリズムが異なってくるので、正規のユーザであっても拒絶されてしまう場合があり、好ましくない。

【００１４】図２に、個人入力データの収集方法の概要を示している。記憶装置５０内に記憶されている制御プログラム（オペレーティングシステム（ＯＳ））は、入力装置１０から入力された入力データ６０を受取り、演算装置２０上で実行中の処理１～３のいずれかのプログラムに渡す。これと並行して、個人入力データ作成処理７０に渡し、個人入力データ５０１を収集する。

【００１５】初めに、キー操作手順の個人差を利用した認証方法の実施形態について説明する。例えば、図３のようにユーザが「じしんがありました」という文章を入力した時、ローマ字入力の場合「ｚｉｓｉｎｎｇａａｒｉｍａｃｉｔａ」とキーボード入力する。ここで、コンピュータにある一定の動作を行わせようとする場合に複数の入力パターンが存在する。この一文ではユーザの認証対象箇所が下線部の引かれた「じ」「し」の３個所が該当する。図４に示すように、かな入力を含めれば「し」は４通り、「じ」は３通りの入力方法がある。ユーザはこのうちのいずれか一つの入力手順を選択しているわけであり、しかも通常ユーザは毎回同じ入力手順でキー操作を行うものと想定される。図５は、このようなキー操作手順の個人差に着目し、認証対象となる文字とユーザのキー入力パターンとの対応関係を定義した認証テーブル５００である。図４で示したように「し」には複数の入力手順が考えられるが、正当なユーザは常にローマ字入力の状態でキーボードの［Ｓ］キー、［Ｉ］キーを順に押下したものとし、他の入力方法では正当なユーザと認識しない。図５では、「じ」「つ」などのその他複数の認証対象となる文字を設定してある。

【００１６】以下、図６のフローチャートを参照して本実施形態の処理を説明する。まず、ユーザ名やユーザＩＤなどのユーザを特定するために問合わせを行い（ステップ６０１）、そのユーザ用の認証テーブル５００が存在するか調べる（ステップ６０２）。

【００１７】図７は、個人入力データがユーザ毎に格納されることを図示したものであり、制御プログラム内８０の個人入力データ作成処理７０は、受け付けた入力を各ユーザの個人入力データとして記憶する。もし存在しなければ、後述する認証テーブル作成処理（ステップ６１４）を行う。図７においては、この処理によって、ユーザＡ，Ｂ，Ｃ毎の個人入力データ５０１Ａ，５０１Ｂ，５０１Ｃが作成されることを示している。なお、図７において、１人のユーザに対し２つのデータファイル（１）、（２）を作成しているが、これは現在の監視時間における入力データを収集して蓄積しておくためと、前回の監視時間における入力データを蓄積しておくためである。

【００１８】次にキーボードからのユーザの入力を受け付けて、その入力情報を個人入力データ５０１として採取していく（ステップ６０３）。これを、あらかじめ定義しておいた所定の監視時間に達するまで繰り返し、個人入力データ５０１を蓄積する（ステップ６０４）。

【００１９】所定の監視時間を経過したならば、蓄積された個人入力データ５０１を用いてユーザ認証を行う。まず、認証対象となる文字を取得したかを判定する（ステップ６０５）。図２を例にして、ユーザが入力した「じしんがありました。」という一文の個人入力データを図８に示す。図５の認証テーブル５００に登録されている情報から、例文中で認証対象となる文字は「じ」１個所「し」２個所の計３個所であり、ここではまず「じ」を取得したものとする。次に、ユーザのキー入力が認証テーブル５００の認証許可入力として登録されているかを判定する（ステップ６０６）。

【００２０】認証対象「じ」は個人入力データのＮｏ１［Ｚ］、２［Ｉ］に該当し、この入力順序は認証テーブル５００に認証許可入力として登録されている。さらに後述する個人入力統計データ比較処理を行い（ステップ６０７）、正当なユーザの入力であるかどうかを照合する（ステップ６０８）。ステップ６０６、ステップ６０８において、不正なユーザと判断された場合、後述する認証失敗処理を行う（ステップ６０９）。

【００２１】全て認証対象に対して認証処理を行うまで、以上の処理を繰り返す（ステップ６１０）。この繰り返し処理の中で「し」の認証も行うが、これに対応する個人入力データは項番３［Ｓ］、４［Ｉ］と項番１４［Ｃ］、１５［Ｉ］である。認証テーブル５００を見ると、認証対象「し」の認証許可入力は［Ｓ］［Ｉ］であり、項番３［Ｓ］、４［Ｉ］は正当なユーザと判定されても、項番１４［Ｃ］、１５［Ｉ］は不正なユーザの入力として認証失敗処理が行われることになる。

【００２２】最後に、ユーザの入力の全てがおわっているかを判定し（ステップ６１１）、そうでなければ、個人入力データを切り替えた後（ステップ６１２）、それまでの個人入力データより個人入力統計データ（図７の７０１Ａ，７０１Ｂ，７０１Ｃ）を作成し（ステップ６１３）、再びステップ６０３へ戻る。これにより、ユーザが文章入力を行う間は、常に入力データが採取され、かつ定期的（所定の監視時間の間隔）に認証処理が実行され続ける。

【００２３】図９に、ステップ６１３の個人入力統計データ作成処理を図示する。個人入力データ５０１を記憶する領域（ファイル）は５０１－１と５０１－２の２つあり、その切替えは本実施形態ではステップ６０４の所定監視時間の経過で行われているが、個人入力データがあらかじめ指定されている記憶容量よりも大きくなったら切り替わるようにしてもよい。切替えが発生して他方の記憶領域に個人入力データ作成が行われるようになると、個人入力統計データ作成処理９０（ステップ６１３）はもう片方の記憶領域に記憶された個人入力データから個人入力統計データ７０１を作成する。個人入力統計データ７０１は、個人入力データを集計したものであ

り、個人入力統計データ比較処理（ステップ６０７）やユーザの入力傾向把握に用いられる。

【００２４】ところで、ステップ６１４の認証テーブル作成処理では、新規ユーザの認証テーブルを作成する。例えば、認証を行わないサンプリング期間を設けて、その間にコンピュータがユーザの入力のログを収集し、そこからユーザ特有の入力パターンを抽出して、認証テーブル５００に登録してもよい。図４の例で言うと、ユーザが「し」を入力する時、必ず［Ｃ］［Ｉ］とキー入力していると判明したならば、これを認証対象入力とすることができる。もちろんユーザがあらかじめ認証テーブル５００に任意に認証対象入力とその入力手順を設定しておいてもよい。

【００２５】次に、ステップ６０７の個人入力データ統計比較処理について述べる。先に行われた認証対象入力の入力順序が認証テーブル５００と合致しても、不正ユーザが正当なユーザの入力を真似て入力を行った可能性がある。そこで、本処理ではさらにキー入力の時間間隔からユーザの認証を行い、認証の正確性を向上させる機能を付加している。

【００２６】図１０は、個人入力データ比較処理の概要を示す図である。ステップ６１３で作成された個人入力統計データ７０１には過去の個人入力データが格納されており、これを元に個人入力統計データ演算処理１００１によって比較用個人入力統計データ１００２を作成し、それを個人入力統計データ比較処理１００３（ステップ６０７）が最新の個人入力データ５０１（ＮＥＷ）と比較することで認証を行う。

【００２７】図１１は比較用個人入力統計データ１００２の詳細例を示す図である。過去のデータから各認証対象入力の最小キー間隔１１０１、最大キー間隔１１０２、平均キー間隔１１０３を算出している。図１１では、「じ」のキー入力［Ｚ］→［Ｉ］間の最小キー間隔＝０．４３、最大キー間隔＝０．７２、平均キー間隔＝０．５５（秒）と算出している。一方、最新の個人入力データである図８を見ると、「じ」に該当する入力Ｎｏ１、２のキー間隔は各入力時刻の差から０．６０をとっているが、平均所要時間０．５５±補正値０．１０が正当なユーザの入力と判定されるから、この場合は正当なユーザと認証する。なお、個人入力統計データ作成処理のたびに比較用個人入力統計データ１００２が更新されるため、ユーザの入力操作の熟練や入力速度の変化に応じて、その値を変化させることができる。

【００２８】また、図１１の補正値１１０４は、図１２に示すような計算方法によってその値が定められる。まず、図１１で示した比較用個人入力統計データ１００２を作成する際に、図１２（ａ），（ｂ）に示すデータを得る。図１２（ａ）のデータとは特定の認証対象入力の過去のキー間隔であり、図１２（ｂ）のデータとは図１２（ａ）のデータを元に作成されたキー間隔の平均値、標準偏差、記録件数である。この図１２（ｂ）のデータをもとにあらかじめ指定しておいた信頼度から図１２（ｃ）に示すような有意水準を求め、さらに有意水準、標準偏差、件数を使って図１２（ｄ）に示すような母集団に対する信頼区間を算出する。この信頼区間が図１１の補正値１１０４となり（図１２（ｅ））、キー間隔の平均値から信頼区間を引いた値から、平均値に信頼区間を足した値までの入力間隔は正規のユーザとみなす。この場合、この補正値１１０４をユーザ自らが設定してもよい。

【００２９】次に、図６のステップ６０９の認証失敗処理について説明する。ステップ６０６、６０８での認証処理に失敗した場合には、不正なユーザにより入力が行われたと判定し、利用を抑止する。例えばユーザに対して警告を発する、パスワードの再入力を要求する、ユーザの処理を強制中断する、処理ができないようにしてユーザアカウントをロックする、などの不正利用対策が考えられる。１回の認証失敗でこのような不正利用対策が実行されるようにしてもよいが、次のような方法もある。

【００３０】図１３は、認証失敗の回数によって不正利用対策をレベル付けした認証失敗テーブル１３００である。認証失敗ポイント１３０３は認証に失敗されるたびに蓄積されていくポイントであり、例えば認証１回の失敗につき１ポイント加算されるとすれば、５回目の失敗ではレベル２の「注意」が不正利用対策として実行される。また、認証１回の失敗につき１ポイントとしなくても、ステップ６０６での認証失敗は３ポイントの加算、ステップ６０８での認証失敗は２ポイントの加算、というようにユーザが任意に設定できる。

【００３１】このように、本実施形態の認証処理は、ユーザの目からは見え難い入力パターンで個人認証を行うため、パスワードやＩＤのように他者に盗まれる可能性が少なく、またあらかじめ認証対象入力をより多く定義しておくことで多数の認証パターンを生成できる。また、この認証はユーザがコンピュータを利用中、あるいは所定のアプリケーション起動中は継続して行われるため、正式ユーザが席を外している間に不正利用者が勝手にコンピュータを利用したとしても、コンピュータはその入力パターンから正式なユーザではないと判断し、その利用を禁止することができる。一方、不正利用者側からはコンピュータがどのような認証を行っているかが見えないわけであるから、不正侵入をあきらめざるをえないという効果が得られる。

【００３２】次に、ユーザのアイコン操作態様から個人認証を行う第２の実施形態について説明する。ある特定の処理を目的としたアイコン操作においても、ほとんどの場合、操作手順が決まっていて、しかも選択可能な入力手順が複数存在する。図１４（ａ）に示す画面１４００を有するアプリケーションプログラムの終了処理で

は、図１４（ｂ）に示すように「メニューバーを用いる」「アイコンメニューを用いる」「右クリックメニューを用いる」「ショートカットキーを用いる」といった方法が存在し、細かく見ればさらに複数の手順が存在する。一口にメニューバーを用いてアプリケーションを終了するといっても、図１４（ｂ）の破線枠内に示すように、①ファイルのプルダウン表示に２パターン、②終了の実行に３パターン、計６パターンの終了方法が存在する。本実施形態は、ユーザがどの操作態様を使用しているかで正当なユーザであるか認証を行うものであり、以下詳しく説明する。

【００３３】図１５は、ユーザの操作態様の個人差によってユーザ認証を行う場合の認証テーブル１５００の例を示す図である。図５の認証テーブル５００が正当なユーザの入力のみを定義していたのに対し、本テーブル１５００では、ある特定の動作や結果に至るための手順の全てを定義している。図１５の例では、アプリケーションの終了処理を行うための全ての操作手順を定義しており、ここに定義されている入力順序以外でアプリケーションの終了はできない。よって、ユーザがアプリケーションを実行した場合には、必ずここに定義された入力手順の一つを実行したことになる。認証許可とは正当なユーザのものと認められる入力手順である。図１５の例では、メニューバーを用いてアプリケーションが終了するのに「ＮＯ．１」と「ＮＯ．３」の手順を用いた場合には正当なユーザと認められ、その他の入力手順では不正なユーザと判定される。

【００３４】以下、図１６のフローチャートを参照して本実施形態の処理を説明する。まず、ユーザの入力を受付けて（ステップ１６０１）、それを個人入力データとして採取した後（ステップ１６０２）、認証対象入力か判定する（ステップ１６０３）。具体的には、図１５の認証テーブル１５００に登録されている各入力手順の「順番１」の内容で認証対象入力かどうかで判定する。例えば、ユーザがアイコンの「ファイル」をマウスで左クリックした場合は、認証テーブル１５００の「ＮＯ．１」、「ＮＯ．２」、「ＮＯ．３」の「手順１」に該当しているため、認証対象入力であると判定する。ユーザの入力が認証対象入力でなければ、個人入力データは破棄して（ステップ１６０４）、判定処理を終える。

【００３５】次に、認証対象入力が終了か否かを判定する（ステップ１６０５）。認証対象入力の終了とは、認証テーブル１５００に登録された入力手順のどれかを完遂した状態のことである。入力手順「ＮＯ．１」、「ＮＯ．２」、「ＮＯ．３」のいずれも「手順１」の後の操作があるから、認証対象入力は終了しておらず、ステップ１６０１へ戻る。

【００３６】そして、再びユーザの入力を受付け、個人入力データを採取し、認証対象入力か否か認証処理を行う（ステップ１６０１～１６０３）。すでに認証対象入力は「ＮＯ．１」、「ＮＯ．２」、「ＮＯ．３」に絞られているから、ユーザの入力がこの３つの入力手順の「順番２」と一致するか否かを判定する。ここでユーザがアイコンの「終了」をマウスで左クリックしていた場合には、「ＮＯ．１」の「順番２」を行ったと判定する。すると、ステップ１６０５でユーザの入力が「ＮＯ．１」を完遂しているとして、認証対象入力は終了と判定し、次のステップへ進む。

【００３７】個人入力データを保存した後（ステップ１６０６）、ユーザの一連の入力が認証テーブル１５００で認証許可されているかを判定する（ステップ１６０７）。認証テーブル１５００の「認証許可」の「○」印は、入力手順「ＮＯ．１」が正当なユーザの入力手順であることを示している。認証許可されていると判定したら、さらに個人入力統計認証データ比較処理で本人との照合を行う（ステップ１６０８）が、これは前記の第１の実施形態と同じである。

【００３８】ステップ１６０８、１６０９において正当なユーザと認証できなかった場合には、前述の実施形態と同様の認証失敗処理を行う（ステップ１６１０）。最後に、ユーザの全入力が終了したかを判定し（ステップ１６１１）、終了するまでステップ１６０１からの処理を繰り返す。

【００３９】図１７は、以上の処理の結果で作成された個人入力データの一例である。本実施形態例によれば、認証対象入力に無関係な入力は蓄積されないので、後の個人入力統計データ作成に便利であり、記憶容量の節約にもなる。

【００４０】次に、操作環境の個人差に着目して個人認証を行う第３の実施形態について説明する。図１８（ａ）～（ｅ）は、ユーザの操作環境の設定手順の例を示す図である。この実施形態では、ユーザは、予め自分が通常使用する操作環境を設定する。図１８では、ブラウザを起動する場合の操作環境を設定する例を示している。まず、コンピュータからの指示により図１８（ａ）の「画面１」が表示され、ここでブラウザを起動する場合の操作環境（あるいは操作環境と操作手順を組み合わせた認証環境）を設定するように指示される。図１８の例では、操作環境と操作手順を組み合わせた認証環境を設定する例を示している。そこで、ユーザは図１８（ｂ）の「画面２」に示すように例えばマウス入力によって①「ＷＷＷ一口メモ」というアプリケーションを開き、この「ＷＷＷ一口メモ」が開かれた操作環境で、②「スタート」メニューを開いて、最後に③ブラウザを選択する、というような設定を行う。次に図１８（ｃ）の「画面３」において「終了」のボタンを押し、さらに図１８（ｄ）に示すような「画面４」でキー間隔の補正値を入力し、最後に図１８（ｅ）に示す「画面５」で「ＯＫ」か否かを応答し、「ＷＷＷ一口メモ」を開いた操作環境におけるブラウザの起動手順の設定を終える。図１

８の例では、ブラウザを開く操作を行っているのであるが、①「WWW一口メモ」というアプリケーションを開き、②「スタート」メニューを開いて、最後に③ブラウザを選択、起動という手順でブラウザを開いている。すなわち、ブラウザを開く際に、「WWW一口メモ」というアプリケーションの開いた操作環境にした後、②③の入力を行わなければ、正当なユーザの入力ではないと判定するような認証手順を設定している。

【００４１】図１９は、図１８におけるユーザの設定手順を元に作成された認証テーブル１９００の例を示すものである。ここで示す認証テーブル１９００は、個人入力データとを１組に構成したものであり、入力順序の方は先の実施形態の認証テーブルと同じであり、個人データの方は先の実施形態個人入力データと同じである。認証処理の流れも先の実施形態で示したものと同じである。認証テーブル１９００は、１人のユーザにつき、アプリケーションプログラム毎に１つずつ作成してもよいし、複数のアプリケーションプログラムを１グループにまとめてグループ単位で作成するようにしてもよい。

【００４２】また、各実施形態では、目的とする結果を得るに至る入力手段の操作手順、操作態様、操作環境をそれぞれ個別に用いた例を挙げたが、これら操作手順、操作態様、操作環境を複数組み合わせてユーザの個人認証を行えるように構成できることはもちろんである。なお、入力装置として、キーボードとマウスを用いたコンピュータに適用した実施の形態を説明したが、その他の入力装置にも同様に適用できる。また、単一のコンピュータに適用した実施の形態を説明したが、ネットワークを介して接続されているコンピュータにおける個人認証方法にも同様に適用できる。また、本発明の認証方法を実施する手順は、認証処理プログラムとしてＣＤ－ＲＯＭ等の記録媒体に格納して汎用のパーソナルコンピュータユーザにインストールして実行できるように構成することができる。

【００４３】

【発明の効果】以上説明したように、本発明によれば、ユーザがコンピュータを使用中にその入力操作手順、操作態様、操作環境の個人差を利用した個人認証を随時行うことにより、セキュリティの高い個人認証を行うことができる。特に、認証済みのユーザが席を離れた場合であっても、第3者による不正使用を抑止することができる。

【図面の簡単な説明】

【図１】本発明を適用したコンピュータシステムの一実施の形態を示すブロック図である。

【図２】個人入力データを収集する方法の説明図である。

【図３】入力手順の個人差を説明するための入力データの例を示す図である。

【図４】図３の入力データに対するキー操作手順の例を示す説明図である。

【図５】キー操作手順の個人差によって個人認証を行う場合の認証テーブルの例を示す図である。

【図６】キー操作手順の個人差によって個人認証を行う場合の認証処理のフローチャートである。

【図７】個人入力データ作成処理によって作成する個人入力データのユーザ別構成図である。

【図８】収集した個人入力データの例を示す図である。

【図９】個人入力データの統計データを作成する手順の説明図である。

【図１０】個人入力統計データから比較用個人入力統計データを作成し、最新の個人入力データと比較する処理の説明図である。

【図１１】比較用個人入力データの例を示す図である。

【図１２】比較用個人入力データの補正値を求める手順を示す説明図である。

【図１３】認証失敗テーブルの例を示す図である。

【図１４】ユーザの操作態様の個人差によって個人認証を行う第２の実施形態の説明図である。

【図１５】ユーザの操作態様の個人差によって個人認証を行う場合の認証テーブルの例を示す図である。

【図１６】ユーザの操作態様の個人差によって個人認証を行う場合の認証手順を示すフローチャートである。

【図１７】ユーザの操作態様の個人差によって個人認証を行う場合の個人入力データの例を示す図である。

【図１８】ユーザの操作環境の個人差によって個人認証を行う場合の認証テーブルの設定手順を示す説明図である。

【図１９】ユーザの操作環境の個人差によって個人認証を行う場合の認証テーブルの例を示す図である。

【符号の説明】

１０…入力装置、２０…演算装置、３０…制御装置、４０…出力装置、５０…記憶装置、１０１…キーボード、１０２…マウス、５００…認証テーブル、５０１…個人入力データ。

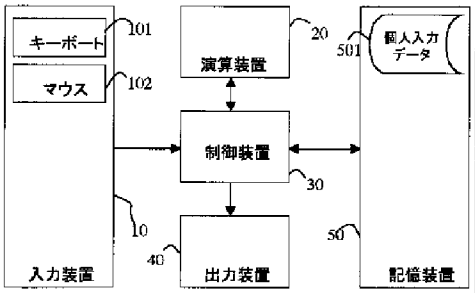
【図３】

図３

じしんがありました。
zi si nn ga a ri ma ci ta

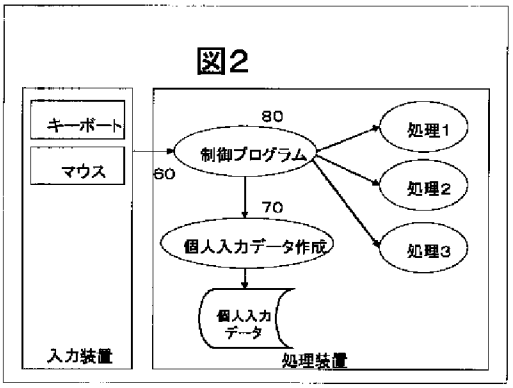
【図１】

図１



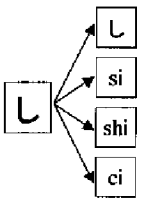
【図２】

図２



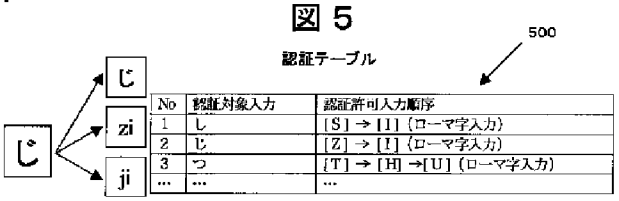
【図４】

図４



【図５】

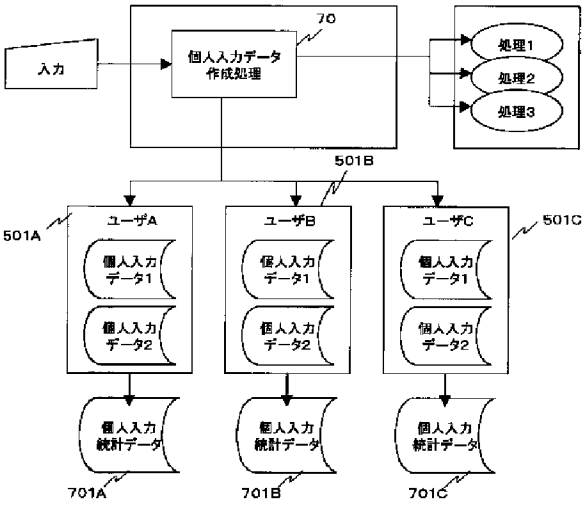
図５



No	認証対象入力	認証許可入力順序
1	し	[S] → [I] (ローマ字入力)
2	じ	[Z] → [I] (ローマ字入力)
3	つ	[T] → [H] →[U] (ローマ字入力)
…	…	…

【図７】

図７



【図８】

図８

個人入力データ

No	入力年月日	入力時刻	ユーザ名	コンピュータ装置名	入力装置名	入力
1	1999/03/03	08:14:30.00	USER1	COMP1	KEY	Z
2	1999/03/03	08:14:30.60	USER1	COMP1	KEY	I
3	1999/03/03	08:14:31.23	USER1	COMP1	KEY	S
4	1999/03/03	08:14:31.82	USER1	COMP1	KEY	I
5	1999/03/03	08:14:32.55	USER1	COMP1	KEY	N
6	1999/03/03	08:14:33.18	USER1	COMP1	KEY	N
7	1999/03/03	08:14:33.80	USER1	COMP1	KEY	O
8	1999/03/03	08:14:34.37	USER1	COMP1	KEY	A
9	1999/03/03	08:14:34.99	USER1	COMP1	KEY	A
10	1999/03/03	08:14:35.74	USER1	COMP1	KEY	R
11	1999/03/03	08:14:36.42	USER1	COMP1	KEY	I
12	1999/03/03	08:14:37.20	USER1	COMP1	KEY	M
13	1999/03/03	08:14:38.91	USER1	COMP1	KEY	A
14	1999/03/03	08:14:39.44	USER1	COMP1	KEY	O
15	1999/03/03	08:14:40.08	USER1	COMP1	KEY	I
16	1999/03/03	08:14:40.67	USER1	COMP1	KEY	T
17	1999/03/03	08:14:41.29	USER1	COMP1	KEY	A
18	1999/03/03	08:14:41.96	USER1	COMP1	KEY	.

【図１１】

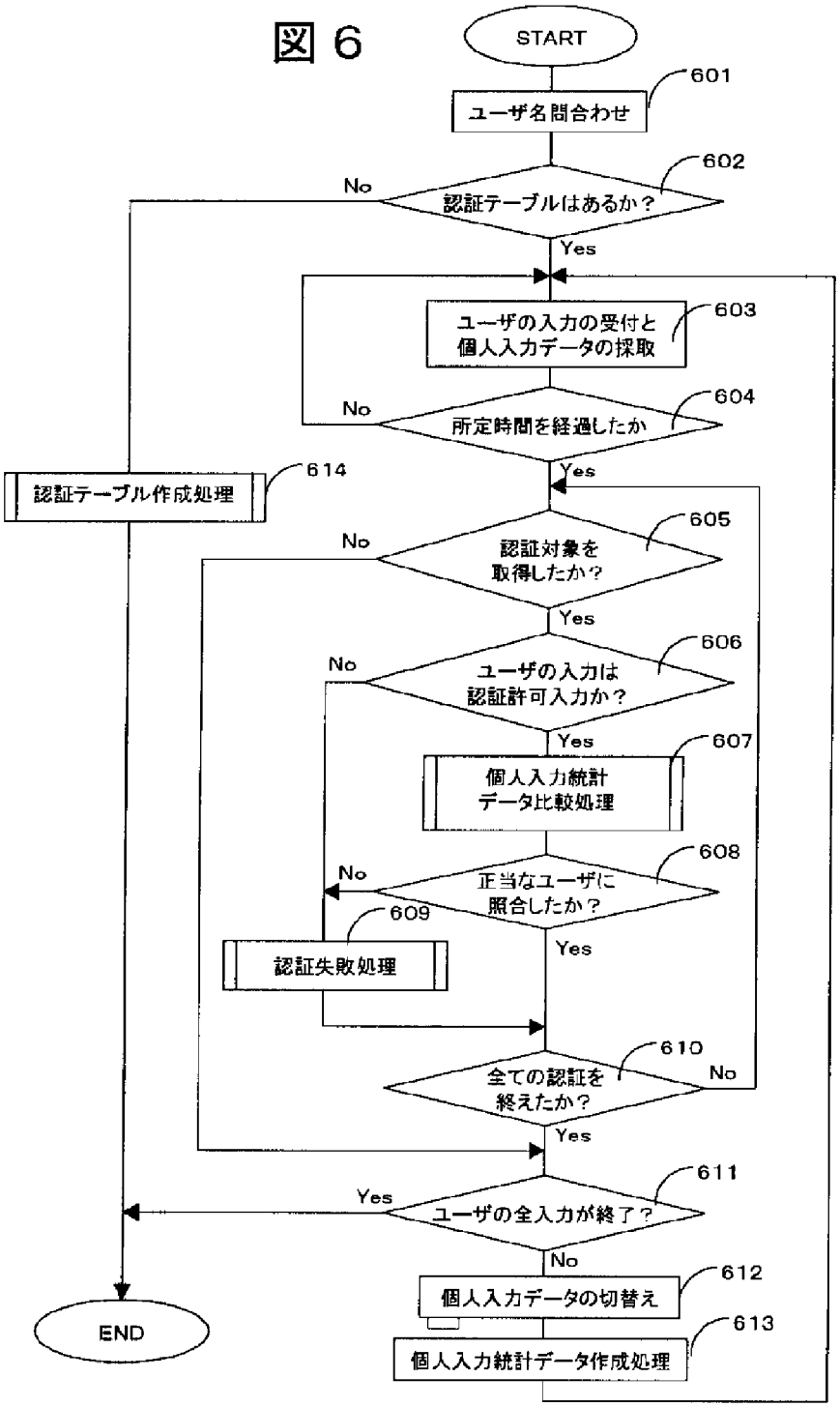
図１１

比較用個人入力データ

認証対象入力	順番	入力キー	最小キー間隔 (1101)	最大キー間隔 (1102)	平均キー間隔 (1103)	補正値 (1104)
じ	1	[Z]	———	———	———	
	2	[I]	0.43	0.72	0.65	0.10
し	1	[S]	———	———	———	
	2	[I]	0.65	1.02	0.72	
つ	1	[T]	———	———	———	
	2	[S]	0.55	0.77	0.62	
	3	[U]	0.40	0.66	0.54	

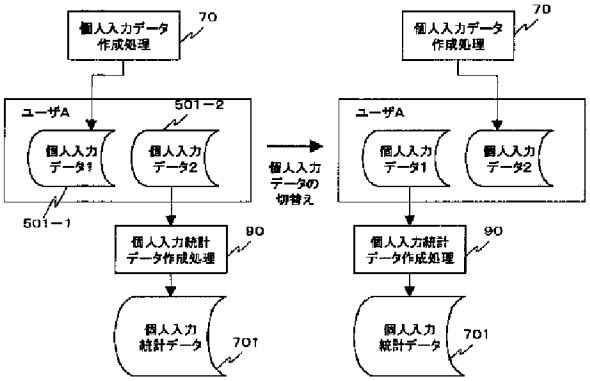
【図6】

図 6


START
601
ユーザ名問合わせ
602
No
認証テーブルはあるか？
Yes
603
ユーザの入力の受付と
個人入力データの採取
604
No
所定時間を経過したか
Yes
614
認証テーブル作成処理
605
No
認証対象を
取得したか？
Yes
606
No
ユーザの入力は
認証許可入力か？
Yes
607
個人入力統計
データ比較処理
608
No
正当なユーザに
照合したか？
609
認証失敗処理
Yes
610
全ての認証を
終えたか？
No
Yes
611
Yes
ユーザの全入力が終了？
No
612
個人入力データの切替え
613
個人入力統計データ作成処理
END

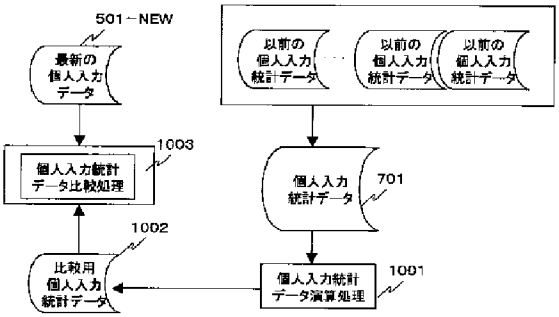
【図9】

図9



【図10】

図10



【図12】

図 12

(a)

項番	打鍵感覚
1	0.400
2	0.500
3	0.600
4	0.500
5	0.550
6	0.550
7	0.600
8	0.450
9	0.400
10	0.550

個人入力データから取得したキー入力の間隔の例

(b)

対象	値
平均	0.510
標準偏差	0.074
件数	10

表1から平均、標準偏差、件数を求める

(c)

項番	対象	値	値
1	信頼度(%)	90%	90%
2	有意水準	0.100	0.100

あらかじめ指定しておいた信頼度から有意水準を求める

(d)

対象	値
信頼区間	0.038

有意水準、標準偏差、件数の使って母集団に対する信頼区間を求める。

(e)

対象	値
平均－信頼区間	0.472
平均＋信頼区間	0.548

上記信頼区間が図9の補正値となる

【図13】

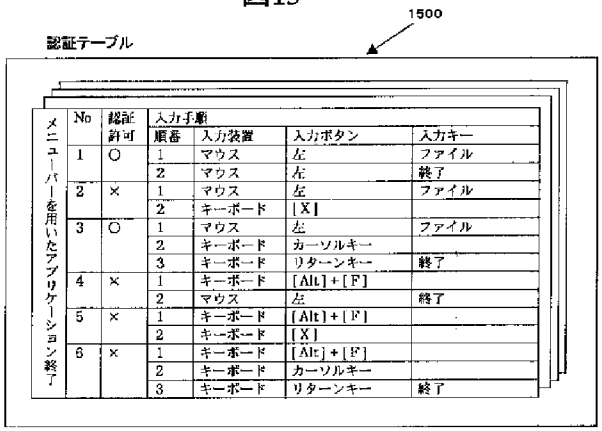
図 13

認証失敗テーブル　1300　1301　1302　1303

レベル	判定結果	内容	認証失敗ポイント
1	正常	正当なユーザと認定できる範囲内であり何も行わない。	1～3 P
2	注意	ユーザに対して「注意」の表示を行う	4～6 P
3	警告	ユーザに対して「警告」の表示とパスワードの再入力を要求する	7～10 P
4	異常	処理を強制中断して、そのユーザアカウントをロックする。	11～ P

【図15】

図15



【図17】

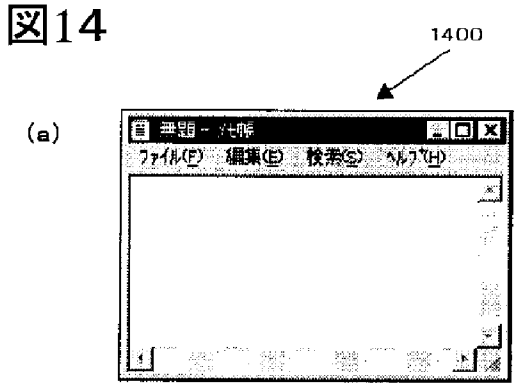
図17

個人入力データ

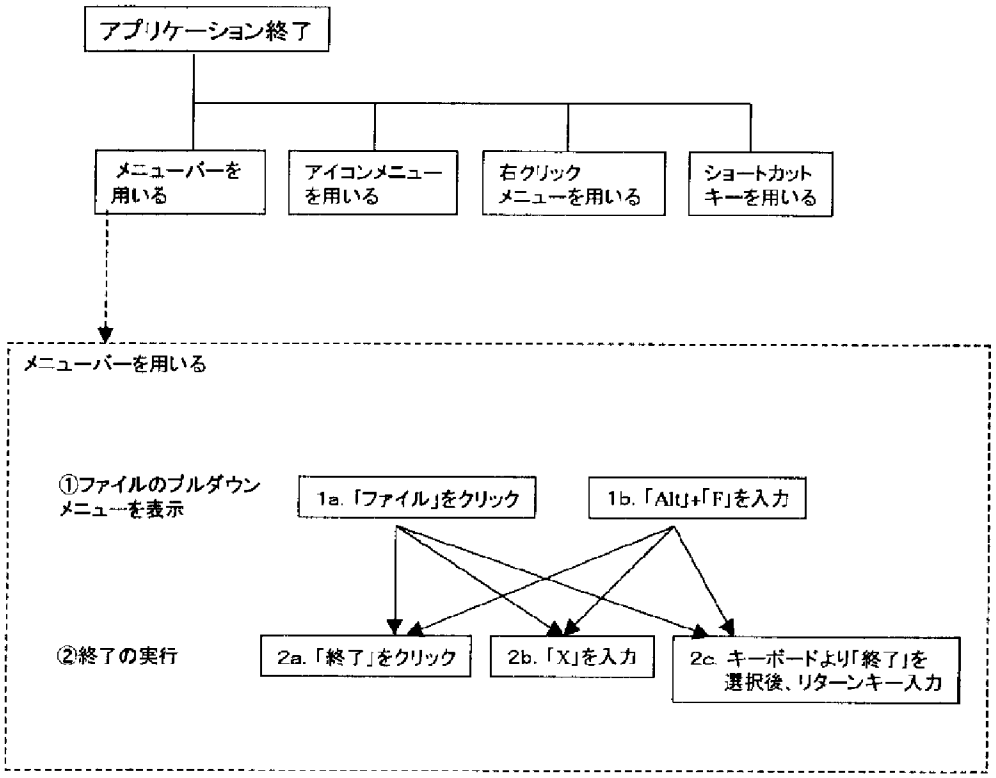
No	入力年月日	入力時刻	ユーザ名	コンピュータ装置名	入力装置名	入力
1	1999/03/03	09:14:30.01	USER1	COMP1	MOU	「ファイル」
2	1999/03/03	09:14:31.90	USER1	COMP1	MOU	「終了」
3	1999/03/03	09:15:00.23	USER1	COMP1	MOU	「ファイル」
4	1999/03/03	09:15:02.22	USER1	COMP1	MOU	「終了」
5	1999/03/03	10:17:22.36	USER1	COMP1	KEY	[Alt]+[F]
6	1999/03/03	10:17:23.87	USER1	COMP1	KEY	[X]
7	1999/03/03	15:22:10.44	USER1	COMP1	MOU	「ファイル」
8	1999/03/03	15:22:12.49	USER1	COMP1	MOU	「終了」
…	…	…	…	…	…	…

【図14】

図14

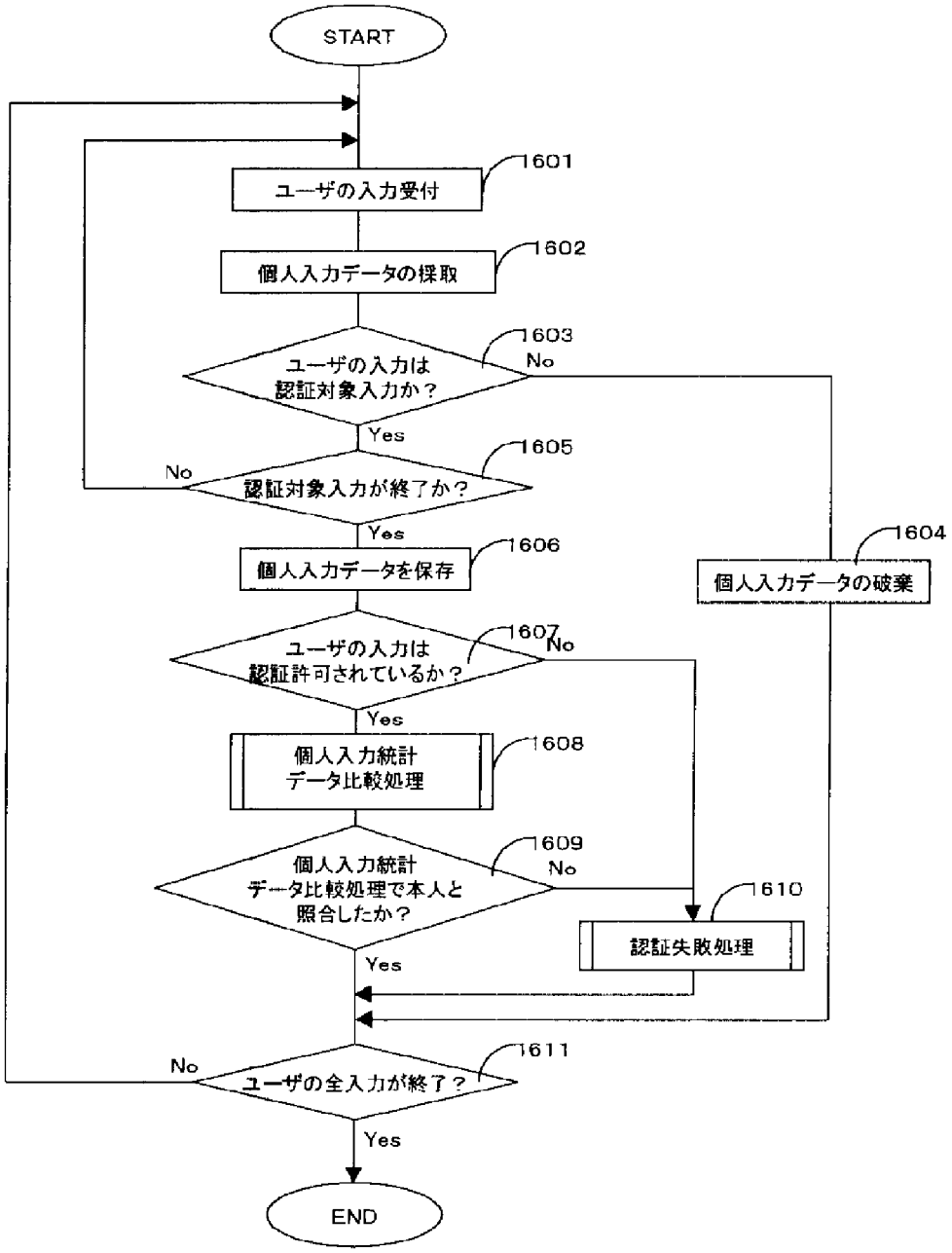


(b)　アプリケーション終了時の操作



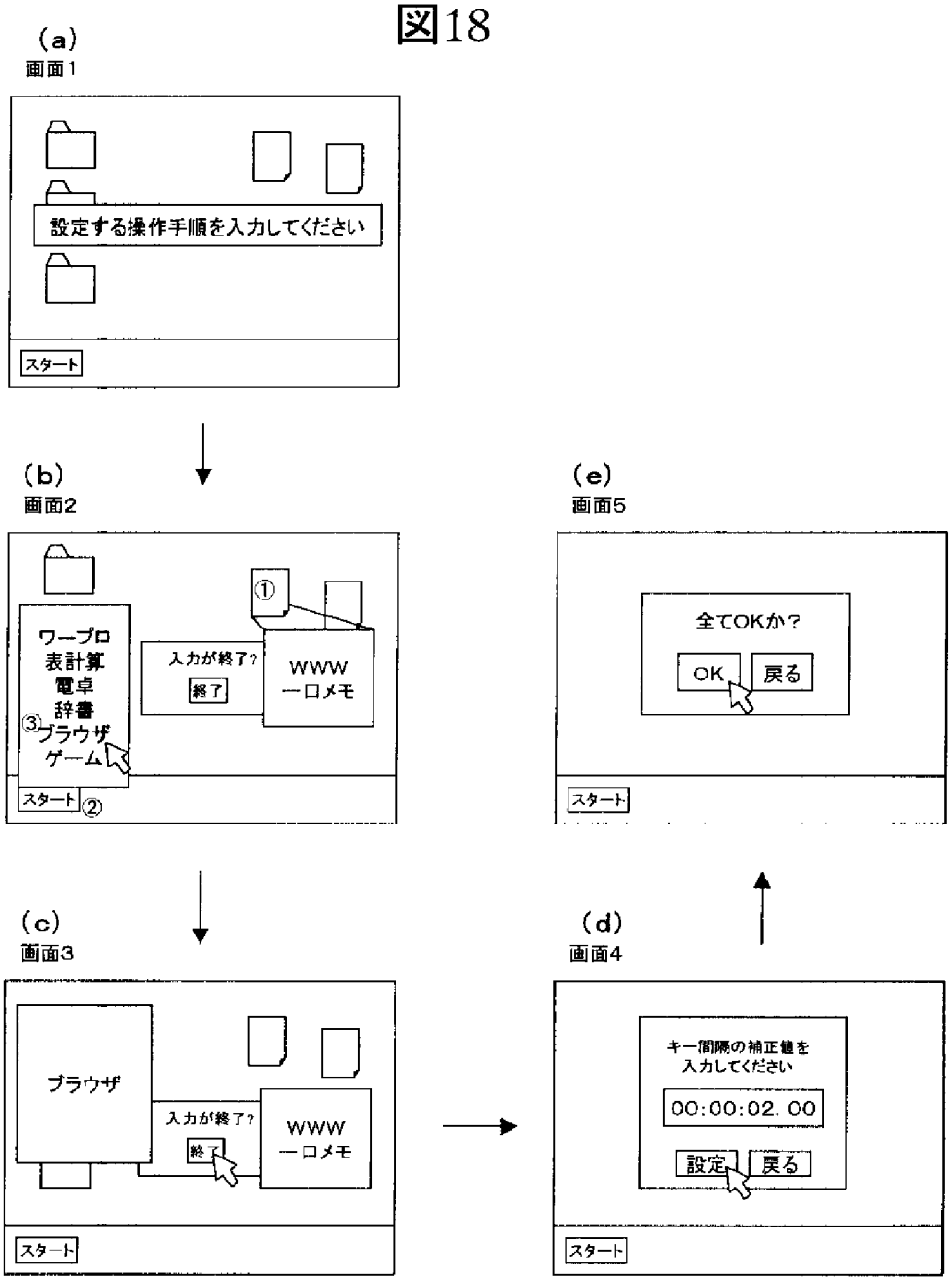
【図16】

図16


START
1601
ユーザの入力受付
1602
個人入力データの採取
1603
ユーザの入力は
認証対象入力か？
No
Yes
1605
No
認証対象入力が終了か？
Yes
1606
個人入力データを保存
1604
個人入力データの破棄
1607
ユーザの入力は
認証許可されているか？
No
Yes
1608
個人入力統計
データ比較処理
1609
個人入力統計
データ比較処理で本人と
照合したか？
No
1610
認証失敗処理
Yes
1611
No
ユーザの全入力が終了？
Yes
END

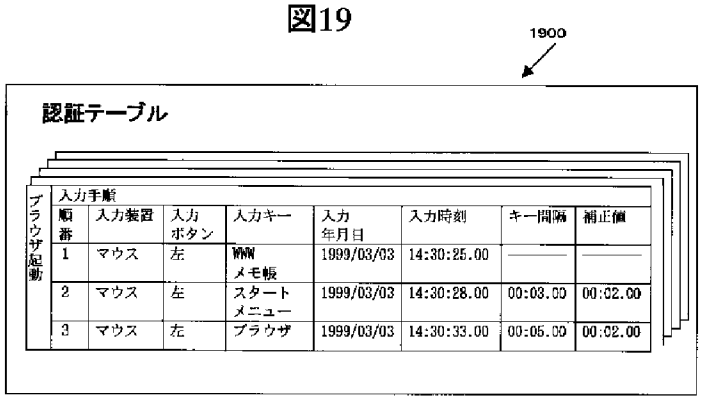
【図18】

図18


(a)
画面1
設定する操作手順を入力してください
スタート
(b)
画面2
ワープロ
表計算
電卓
辞書
③ブラウザ
ゲーム
スタート
②
①
入力が終了?
終了
WWW
一口メモ
(c)
画面3
ブラウザ
入力が終了?
終了
WWW
一口メモ
スタート
(d)
画面4
キー間隔の補正値を
入力してください
00:00:02.00
設定
戻る
スタート
(e)
画面5
全てOKか?
OK
戻る
スタート

【図１９】

図19


1900
認証テーブル
ブラウザ起動
入力手順
順番
入力装置
入力ボタン
入力キー
入力年月日
入力時刻
キー間隔
補正値
1 マウス 左 WWW メモ帳 1999/03/03 14:30:25.00
2 マウス 左 スタートメニュー 1999/03/03 14:30:28.00 00:03.00 00:02.00
3 マウス 左 ブラウザ 1999/03/03 14:30:33.00 00:05.00 00:02.00